

SISTEM APLIKASI KRIPTOGRAPHY ADVANCED ENCRIPTION STANDARD

Laporan Penelitian



Disusun oleh:

Heri Santoso, M.Kom

NIDN. 0119116701

**PROGRAM STUDI ILMU KOMPUTER
FAKULTAS SAINS DAN TEKNOLOGI
UIN SUMATERA UTARA MEDAN**

2017

LEMBAR PENGESAHAN

Judul Penelitian **SISTEM APLIKASI RIPTOGRAPHY
ADVANCED ENCRYPTION
STANDARD**

Bidang Ilmu : Teknologi Informatika
Topik Unggulan : Komputasi

Ketua Peneliti

a. Nama Lengkap : Heri Santoso, M.Kom

b. NIDN : 0119116701

c. Jabatan Fungsional / : Asisten Ahli

d. Fakultas/Jurusan : Fakultas Sains dan Teknologi

e. Pusat Penelitian : Prodi Ilmu Komputer

f. Alamat Institusi : Kampus 1 UIN Sumatera Utara Medan

g. Telpon/Faks/E-mail : Jln. IAIN No.1, Medan 20235

h. Lama Penelitian : 082167005000 / Herisantoso@uinsu.ac.id

i. Lama Penelitian Keseluruhan : 3 Bulan

i. Biaya Penelitian yang dihabiskan : Dana mandiri Rp. 3.000.000,-

Mengetahui,
Kaprodi Ilmu Komputer

Medan, September 2017
Ketua Peneliti,

Mhd Furqan, S.Si., M.Comp.Sc.
NIDN. 2006078003

Heri Santoso, M.Kom
NIDN. 0119116701

KATA PENGANTAR

Segala puji bagi Allah SWT yang senantiasa memberikan taburan rahmat dan karunia-NYA sehingga penulis dapat menyelesaikan laporan penelitian yang berjudul : **“SISTEM APLIKASI KRIPTOGRAPHY ADVANCED ENCRYPTION STANDARD”**.

Penulisan Laporan Penelitian ini dilakukan dalam rangka melengkapi kewajiban menjadi seorang Dosen dalam melaksanakan Tri Dharma Perguruan Tinggi. Penulis menyadari sepenuhnya bahwa dalam penulisan Penelitian banyak pihak yang membantu dan berpartisipasi. Untuk itu ucapan terima kasih khususnya penulis ucapkan kepada :

1. Bapak Dr. H. M. Jamil, M.A selaku Dekan Fakultas Sains dan Teknologi UIN Sumatera Utara Medan.
2. Bapak Mhd Furqan, S.Si., M.Comp.Sc., selaku Ketua Program Studi Ilmu Komputer Fakultas Sains dan Teknologi UIN Sumatera Utara Medan
3. Teman-teman Dosen yang telah membantu pelaksanaan penelitian ini.
4. Teman-teman Staf Laboratorium yang turut membantu atas terselesaikannya penelitian ini.

Atas semua jasa tersebut, penulis serahkan kepada Allah SWT, semoga dibalas dengan Rahmat yang berlipat ganda. Walaupun Penelitian ini telah tersusun dengan sebaik mungkin, penulis tetap mengharapkan kritik dan saran yang membangun untuk penyempurnaan penelitian ini. Semoga penelitian ini dapat berguna bagi kita semua dan bagi penulis sendiri khususnya.

Medan, September 2017

Peneliti,

Heri Santoso, M.Kom

DAFTAR ISI

LEMBAR PENGESAHAN

KATA PENGANTAR	i
ABSTRAK	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	viii
DAFTAR TABEL	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian	4
1.7 Sistematika Penulisan	4

BAB II LANDASAN TEORI

6

2.1 Citra Digital	6
2.1.1 Format <i>File</i> Citra JPEG/JPG	7
2.1.2 Format <i>File</i> Citra PNG	8
2.1.3 Format <i>File</i> Citra GIF	8

2.2	Kriptografi	9
2.2.1	Algoritma Kriptografi	10
2.2.2	Algoritma Kunci Asimetri	11
2.2.3	Algoritma Kunci Simetri	12
2.2.4	Tipe dan Mode Algoritma Kunci Simetri	13
2.3	Algoritma Rijndael	14
2.3.1	Proses Enkripsi Algoritma Rijndael (AES)	17
2.3.2	Proses Dekripsi Algoritma Rijndael (AES)	23
2.3.3	Ekspansi Kunci	25
2.4	Rekayasa Perangkat Lunak (<i>Software Engineering</i>)	25
2.5	Analisis dan Perancangan Sistem	26
2.6	UML (<i>Unified Modelling Language</i>)	26
2.7	Bahasa Pemrograman Java	29
BAB III ANALISIS DAN PERANCANGAN SISTEM		31
3.1	Analisis Masalah	31
3.1.1	Analisis Aplikasi Perangkat lunak	31
3.1.2	Analisis Layanan Kriptografi	31
3.1.3	Analisis Algoritma Kriptografi	32
3.1.3.1	Pembangkitan Kunci	33
3.1.3.2	Proses Enkripsi	39
3.1.3.3	Proses Dekripsi	42
3.1.4	Analisis Keamanan <i>File</i> Citra	44
3.2	Analisis Kebutuhan Perangkat Lunak	45

3.2.1	Dekripsi Umum	45
3.2.2	Spesifikasi Kebutuhan Perangkat Lunak	45
3.2.3	Model <i>Use Case</i>	47
3.2.3.1	Aktor dan Tujuan	47
3.2.3.2	Diagram <i>Use Case</i>	47
3.2.3.3	Skenario <i>Use Case</i>	48
3.2.3.4	<i>Activity</i> Diagram	50
3.2.4	<i>Flowchart</i> Algoritma Rijndael	53
3.3	Perancangan Perangkat Lunak	55
3.3.1	Perancangan Antar Muka	55
BAB IV IMPLEMENTASI DAN HASIL		58
4.1	Implementasi	58
4.1.1	Perangkat Lunak	58
4.1.2	Perangkat Keras	59
4.2	Pengujian Aplikasi	59
4.2.1	Tampilan Menu Utama	59
4.2.2	Tampilan Menu Enkripsi	60
4.2.3	Tampilan Menu Dekripsi	62
4.2.4	Tampilan Menu Biodata.....	63
4.3	Hasil	64
4.3.1	Kelebihan dan Kekurangan Aplikasi	65
BAB V KESIMPULAN DAN SARAN		66

5.1	Kesimpulan	66
5.2	Saran	67

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Dekripsi	11
Gambar 2.2 Algoritma Kunci Asimetri	12
Gambar 2.3 Algoritma Kunci Simetri	12
Gambar2.4 Ilustrasi <i>Array State</i>	16
Gambar 2.5 Ilustrasi Pengisian <i>Array State</i>	16
Gambar 2.6 Diagram Proses Enkripsi Algoritma Rijndael	17
Gambar 2.7 Ilustrasi Transformasi <i>SubBytes</i>	19
Gambar 2.8 Hasil Transformasi <i>SubBytes</i>	19
Gambar 2.9 Ilustrasi Transformasi <i>Shiftrows</i>	19
Gambar 2.10 Ilustrasi Perkalian Matriks <i>MixColumn</i>	20
Gambar 2.11 Ilustrasi Transformasi <i>MixColumn</i>	21
Gambar 2.12 Hasil Transformasi <i>MixColumn</i>	21
Gambar 2.13 Ilustrasi Transformasi <i>AddRoundKey</i>	22
Gambar 2.14 Hasil Transformasi <i>AddRoundKey</i>	22
Gambar 2.15 Diagram Proses Dekripsi Algoritma Rijndael	23
Gambar 3.1 <i>Array</i> Kunci	34

Gambar 3.2 Proses <i>Array</i>	34
Gambar 3.3 <i>Rot Word</i>	35
Gambar 3.4 Hasil <i>SubBytes</i>	35
Gambar 3.5 Proses Pengisian Kolom Ke-1 pada <i>Round Key</i> Pertama	36
Gambar 3.6 Hasil <i>Round Key</i> Kolom Ke-1	36
Gambar 3.7 Hasil <i>Round Key</i> Kolom Ke-2	37
Gambar 3.8 Hasil <i>Round Key</i> Kolom Ke-3	37
Gambar 3.9 Hasil <i>Round Key</i> Kolom Ke-4	38
Gambar 3.10 Hasil <i>Round Key</i> 1	38
Gambar 3.11 Hasil Seluruh <i>Round Key</i>	39
Gambar 3.12 Diagram Proses Enkripsi Rijndael	40
Gambar 3.13 Diagram Proses Dekripsi Rijndael	42
Gambar 3.14 Diagram <i>Use Case</i>	47
Gambar 3.15 <i>Activity</i> Diagram Enkripsi	51
Gambar 3.16 <i>Activity</i> Diagram Dekripsi	52
Gambar 3.17 <i>Flowchart</i> Proses Enkripsi Algoritma Rijndael	53
Gambar 3.18 <i>Flowchart</i> Proses Dekripsi Algoritma Rijndael	54

Gambar 3.19 Rancangan Tampilan Menu Utama	55
Gambar 3.20 Rancangan Tampilan Menu Enkripsi	56
Gambar 3.21 Rancangan Tampilan Menu Dekripsi	57
Gambar 3.22 Rancangan Tampilan Menu Biodata	57
Gambar 4.1 Tampilan Menu Utama	60
Gambar 4.2 Tampilan Menu Enkripsi	61
Gambar 4.3 Tampilan <i>File</i> Citra yang akan di Enkripsi	61
Gambar 4.4 <i>Message Box</i> Nama <i>File</i> Enkripsi	62
Gambar 4.5 Tampilan Menu Dekripsi	62
Gambar 4.6 Tampilan <i>File</i> Citra yang akan di Dekripsi	63
Gambar 4.4 <i>Message Box</i> Nama <i>File</i> Dekripsi.....	63
Gambar 4.8 Form Menu Biodata	64

DAFTAR TABEL

Tabel 2.1 Perbedaan Kunci Rijndael	15
Tabel 2.2 <i>S-Box</i> Rijndael	18
Tabel 2.3 Tabel <i>inverse S-Box</i> dalam Transformasi <i>InvByteSub</i>	24
Tabel 3.1 Aktor dan Tujuan	47

Tabel 3.2 Skenario <i>Use Case</i> Enkripsi	48
Tabel 3.3 Skenario <i>Use Case</i> Dekripsi	50

ABSTRAK

Citra digital merupakan salah satu data atau informasi yang sering disalahgunakan, oleh karena itu untuk menjaga keamanan dan kerahasiaan suatu data citra digital menjadi hal yang penting. Salah satu pengamanan bisa dilakukan dengan menerapkan algoritma Rijndael. Empat proses utama algoritma ini terdiri dari satu proses permutasi(*ShiftRows*) dan tiga proses substitusi (*SubBytes*, *MixColumns*, dan *AddRoundKey*) dan juga proses penjadwalan kunci. Dalam penelitian ini akan dibahas tentang pengamanan citra digital dengan algoritma Rijndael dan juga implementasi algoritma ini dalam mengamankan citra digital. Algoritma Rijndael terdapat dalam proses enkripsi dan dekripsi yang dapat diaplikasikan untuk pengamanan citra digital. Hasil dari aplikasi ini mampu mengenkripsi dan mendekripsi *file* citra tanpa mengubah integritas data dari *file* citra tersebut.

Kata Kunci : Citra Digital, Algoritma Rijndael, Enkripsi, Dekripsi